

REMARKS/ARGUMENTS

Claims 2-4, 6-8 and 10-12 are pending in the present application. Claims 10 and 12 have been amended by this Amendment. Claims 1, 5 and 9 have been previously canceled without prejudice or disclaimer.

Claim Rejections under 35 USC § 103

Claims 2-4, 6, 7, and 10-12 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent 6,505,215 (“Kruglikov”) in view of U.S. Patent 6,824,064 (“Guthery”), and further in view of U.S. Patent 6,779,002 (“Mwaura”).¹ Claim 8 stands rejected under 35 USC § 103(a) as unpatentable over Kruglikov in view of Guthery, Mwaura, and U.S. Patent 6,676,022 (“Guthery ‘022”).

Applicants’ disclosed embodiments are directed to the synchronization of a database contained in a mobile first data processing system with another database contained in a network operator server (i.e. the “second data processing system”). In accordance with the invention, an operator or network-supplied application is loaded into a security token, such as a SIM card, that is coupled to the mobile first data processing system. The application is operable to request that the mobile first data processing system start a synchronization process between the database stored in the mobile first data processing system and the database stored in the network operator server in accordance with a specific operator/network synchronization policy.

The security token does not contain the database, i.e., the application and the database are separate and located in different devices. In other words, the application loaded in the security token provides a remote command to the mobile first data processing system to start the

¹ The Office Action, at page 6, erroneously includes claims 8 and 9 in the statement of this rejection. Claim 8 was rejected on other grounds, and Claim 9 was previously canceled.

synchronization process. The security token is thus a third party to a system that includes the mobile first data processing system and the network operator server. A user of the mobile first data processing system cannot start or initiate synchronization for any database in the mobile first data processing system because such control is located remotely, in the application in the security token, from the mobile first data processing system (which contains the database). Synchronization is instead started automatically by the security token, which does not contain the database.

To clarify this aspect of the invention, independent claim 10 now recites, *inter alia*, “a first database that is stored in a mobile first data processing system” and “loading an application into a security token coupled to the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy”. Independent claim 12 similarly recites these features.

Kruglikov discloses a system for synchronizing a portable system (110), e.g., a handheld device, with a personal computer (150). The Examiner concedes that Kruglikov does not disclose “a security token coupled to the mobile first data processing device, loading the application in the security token,” but purportedly finds “an application in the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy.” (See final Office Action at page 4).

However, the portions of Kruglikov cited by the Examiner disclose only user-initiated synchronization, i.e., synchronization which is initiated locally by a user by placing the portable system in a cradle (see, e.g., col. 4, lines 35-38). Moreover, the Examiner acknowledges that the

application for synchronization in Kruglikov is located in the same data processing system that stores the database. In other words, the application in Kruglikov is not remotely coupled to the portable computer system that stores the database, and the synchronization in Kruglikov is not initiated by a remote command. The Examiner has not identified anything in Kruglikov that teaches or suggests “a first database that is stored in a mobile first data processing system” and “loading an application into a security token coupled to the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy”, as recited in Applicants’ independent claims 10 and 12.

The Examiner further cites Guthery as purportedly teaching “a security token coupled for communication with the mobile first data processing system and an application being loaded into the security token.”

Guthery relates to a smart card capable of storing a number of applications and a memory that is logically partitioned into a number of memory blocks. Guthery’s system seeks to allow simultaneous communication with more than one of the applications. To do so, it is necessary to dynamically allocate the scarce memory of the smartcard. This is done using a control program stored on the smartcard. (See Abstract of Guthery and col. 2, lines 52-58).

Guthery does not address database synchronization and, therefore, does not teach or suggest “a first database that is stored in a mobile first data processing system” and “loading an application into a security token coupled to the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy”, as recited in Applicants’ independent claims 10 and 12. Guthery,

therefore, does not remedy the deficiencies of Kruglikov, discussed above, with respect to these claimed features.

The Examiner contends that Guthery broadly teaches “loading the application in the security token.” However, Guthery does not teach that any application can or should be loaded into the smartcard, as the Examiner suggests. Rather, Guthery simply teaches the use of multiple conventional security-related applications on a smart card, such as for use with credit card terminals, automated teller machines (ATMs), and mobile phones, with the additional inclusion on the smart card of a memory administration program that allows simultaneous communication with these various applications while dynamically allocating the smartcard’s scarce memory:

The present invention provides tight linkage between the communication with smart card applications, allocation of scarce resources within the smart card, and the scheduling of execution of those applications. The system and method is constructed to embrace and be compatible with current modes of smart card usage.

(Guthery at col. 7, lines 36-42).

Therefore, even assuming, *arguendo*, that Kruglikov discloses the claimed application “operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy,” as the Examiner contends, the combination of Kruglikov and Guthery would not teach or suggest a first database that is stored in a portable system remote from a synchronization program loaded into the smartcard, or that a remote command is provided to the portable system from the smart card to start the synchronization process. Rather, this combination of references would, at most, teach the use of a smartcard as a security device, with the synchronization program being stored on the portable system, rather than in the smartcard because that is where Kruglikov expressly teaches

that the synchronization program is stored, and Guthery fails to provide any teaching with respect to such a synchronization program.

Moreover, Guthery describes a plurality of applications that are run at the same time. In contrast, Applicants' claimed invention is directed to only a single application that transmits "a command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested". It is only after this synchronization that the mobile first data processing system, which stores the first database remotely from the application, initiates "the synchronization process of the first and second databases in response to receiving the command".

The third cited reference, Mwaura, discloses a computer software framework and method for synchronizing data across multiple databases involving the exchange of data synchronization messages. The Examiner cites Mwaura as purportedly teaching receiving a message by an application and determining if synchronization is needed by checking whether the message is relevant and, if so, taking a synchronization action. However, nothing has been found in Mwaura that would remedy the deficiencies of the combination of Kruglikov and Guthery with respect to the features of independent claims 10 and 12 discussed above.

Therefore, the Examiner's *prima facie* case in support of the rejection of independent claims 10 and 12 suffers from the additional deficiency that the cited references do not disclose the claimed feature: "a first database that is stored in a mobile first data processing system" and "loading an application into a security token coupled to the mobile first data processing system, the application being operable to request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy".

Independent claims 10 and 12 are accordingly deemed to be patentably distinct over the cited art for at least the foregoing reasons.

Regarding motivation to combine the cited references, the Examiner, citing Guthery, asserts:

[I]t would have been obvious to a person of ordinary skill in the art . . . to modify the teachings of Kruglikov with the teachings of Guthery to have a data processing system include a security token controlled by an operator and load an application into the security token to move the administration of simultaneous communication with multiple applications on a smart card into the smart card itself.

(Office Action at pages 4-5, emphasis added). However, the rationale offered by the Examiner merely addresses why one of ordinary skill in the art would have: (1) combined a smart card security device with Kruglikov's portable system; and (2) included a multiple-application administration program on the smart card itself. The Examiner's rationale does not address why one of ordinary skill in the art would have loaded a portable/remote database synchronization program into the smart card.

Therefore, the *prima facie* case in support of the rejection of independent claims 10 and 12 suffers from the additional deficiency that the Examiner has failed to show proper motivation for the proffered combination and modification of the cited references necessary to support the rejections.

In view of the above, it is submitted that *prima facie* obviousness has not been established with respect to Independent claims 10 and 12.

Accordingly, it is requested that the rejection of independent claims 10 and 12 under 35 U.S.C. § 103, and of all of the claims depending from these claims, be withdrawn.

CONCLUSION

In view of the foregoing, reconsideration, and withdrawal of all rejections, and allowance of all pending claims, are respectfully solicited.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: April 23, 2010